CIRT-Level Response to Advanced Persistent Threat

Richard Bejtlich
Director of Incident Response, General Electric
richard@taosecurity.com
taosecurity.blogspot.com
Introduction

• Bejtlich ("bate-lik") biography
  – General Electric, (07-present)
  – TaoSecurity (05-07)
  – ManTech (04-05)
  – Foundstone (02-04)
  – Ball Aerospace (01-02)
  – Captain at US Air Force CERT (98-01)
  – Lt at Air Intelligence Agency (97-98)

• Author
  – Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  – Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  – Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  – Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
Assumptions

• You are an APT victim.
• You care.
• You have hope.

Remember Red, hope is a good thing, maybe the best of things, and no good thing ever dies...

I hope I can make it across the border. I hope to see my friend and shake his hand. I hope the Pacific is as blue as it has been in my dreams.

I hope.

- Andy, The Shawshank Redemption
Critical Themes

• Prevention eventually fails.
• Persistent threats never give up.
• Winning does not mean preventing compromise. Rather:
  – Increase $/MB
  – Predict next move
  – Track adversary change
  – Intrusion suppression
Favorite Kris Harms APT Quotes (FIRST 2010)

• “Compliance is the floor upon which you’re going to fall when you get hacked.”
• “Today a B [grade] is not good enough.”
• “Do not get in a battle over knowledge of Windows with an intruder. You will lose.”
• “Lesley Stahl, I pwn your wireless.”

http://www.cbsnews.com/video/watch/?id=3538299n
First Hour after D-Zero

• Document everything.
• Change communication patterns.
• Activate your IR plan.
First Day after D-Zero

- Switch to alternative computing platforms.
- Implement trustworthy communication.
- Inventory security data.
First Week after D-Zero

- Decide to enlist external help.
- Deliver initial briefing to decision makers.
- Analyze available security evidence.
- Begin deploying additional instrumentation.

D-Zero + 1 week
First Month after D-Zero

- Determine incident scope.
- Evaluate effectiveness of security instrumentation.
- Plan remediation.
First Year after D-Zero

- Evaluate IR capability effectiveness
- Institutionalize counter-APT ops.
- Develop and embed counter-APT improvements.
- Collaborate with peers.
- Expand security instrumentation.
- Hire help.

D-Zero + 1 year
Second Year after D-Zero

- Create Red-Blue Team.
- Develop security intelligence capability.
- Contribute to industry counter-APT work.
- Continue hiring help.
Containment vs Honeynet?

• Reasons to *not* immediately contain/disconnect victims *when you are new to counter-APT ops*:
  
  – Scope of incident likely unknown.

  – Disconnecting victims removes intelligence source.

  – Adversary will notice and change tools, tactics, and procedures.

• When to start disconnecting? *When you meet your win criteria.*
Suggested CIRT Structure
Hiring Priorities

- **Incident Handlers** - subject matter experts who will establish early credibility and competency
- **Event Analysts** - 24x7 coverage to support more routine work
- **Incident Analysts** - assume the natural balance between IH and EA work
- **Support team** - transfer design, build, and run activities from the IRC to Support
- **Threat cell** - profile adversaries and professionalize reporting
- **Blue team** - provide collaborative assessment assistance
- **Technical Assistance Group** - internal security consulting
- **Incident Coordinator** - quality control for IRC operations
- **Red team** - adversary replication and simulation
### Peer incident detection and response teams

<table>
<thead>
<tr>
<th>Company</th>
<th>Team Name</th>
<th>Employees</th>
<th>Team FTE</th>
<th>Contractors</th>
<th>FTE per EC</th>
<th>FTE + Contractor per EC</th>
<th>CIRT FTE per 10,000 employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Electric</td>
<td>GE-CIRT</td>
<td>296,000</td>
<td>12</td>
<td>3</td>
<td>.000041</td>
<td>.000051</td>
<td>0.41</td>
</tr>
<tr>
<td>Aerospace 1 1</td>
<td>IRT</td>
<td>XXX,000</td>
<td>11</td>
<td>0</td>
<td>.000073</td>
<td>.000073</td>
<td>0.73</td>
</tr>
<tr>
<td>Aerospace 2 1</td>
<td>NOSC / SecEng</td>
<td>XX,000</td>
<td>13</td>
<td>0</td>
<td>.000289</td>
<td>.000289</td>
<td>2.89</td>
</tr>
<tr>
<td>DIB 1 1</td>
<td>Sec Ops</td>
<td>XXX,000</td>
<td>11</td>
<td>1</td>
<td>.000088</td>
<td>.000096</td>
<td>0.88</td>
</tr>
<tr>
<td>DIB 2 1</td>
<td>CSIRT</td>
<td>XX,000</td>
<td>5</td>
<td>2</td>
<td>.000076</td>
<td>.000106</td>
<td>0.76</td>
</tr>
<tr>
<td>DIB 3 1</td>
<td>DIB3-CIRT</td>
<td>XXX,000</td>
<td>50</td>
<td>0</td>
<td>.000345</td>
<td>.000345</td>
<td>3.44</td>
</tr>
<tr>
<td>DIB 4 1</td>
<td>DIB4CERT</td>
<td>XX,000</td>
<td>42</td>
<td>2</td>
<td>.000575</td>
<td>.000603</td>
<td>5.75</td>
</tr>
<tr>
<td>Aerospace 3 1</td>
<td>IRT</td>
<td>X,000</td>
<td>2</td>
<td>0</td>
<td>.000500</td>
<td>.000500</td>
<td>5</td>
</tr>
<tr>
<td>Silicon Valley 1 3</td>
<td>CIRT</td>
<td>XX,000</td>
<td>24</td>
<td>0</td>
<td>.000366</td>
<td>.000366</td>
<td>3.66</td>
</tr>
<tr>
<td>Software Company 1 3</td>
<td>IRT</td>
<td>XX,000</td>
<td>41</td>
<td>0</td>
<td>.000442</td>
<td>.000442</td>
<td>4.42</td>
</tr>
<tr>
<td>Software Company 2 2</td>
<td>Sec Ops Center</td>
<td>X,000</td>
<td>15</td>
<td>0</td>
<td>.001875</td>
<td>.001875</td>
<td>18.75</td>
</tr>
<tr>
<td>Utility Company 1 2</td>
<td>Sec Ops Center</td>
<td>XX,000</td>
<td>16</td>
<td>0</td>
<td>.000800</td>
<td>.000800</td>
<td>8</td>
</tr>
</tbody>
</table>

5 IR per 10,000 employees

- Average FTE per EC (AFPE): .000456
- Average FTE + Contractor per EC (AFCPE): .000462
- Implied GE-CIRT FTE for GE based on AFPE: 134 FTEs
- Implied GE-CIRT FTE for GE based on AFCPE: 136 FTEs

Sources
- 2009 DSIE survey 1
- 2008 EIMP project 2
- 2009 EIMP project 3
Incident Cycle

Plan
- Prepare
- Assess
- Security Tasks

Resist
- Filter
- Protect

Detect
- Collect
- Analyze
- Escalate
- Resolve

Respond
- Incident Handlers
- Business Response Teams
- Red-Blue Team

Note: GE-CIRT Components

Incident Response Center

IT and Security Teams
- Technical Assistance Group
- Threat Cell

Event Analysts
- Incident Analysts

Security Project Managers
Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

Richard Bejtlich
richard@taosecurity.com
taosecurity.blogspot.com